What is Claimed is:

1. A system for generating computer security threat management information, comprising:

a Threat Management Domain Controller (TMDC) that is responsive to a computer-actionable Threat Management Vector (TMV), the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat, a second computer-readable field that provides identification of a release level for the system type, and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level, the TMDC being configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems.

2. A system according to Claim 1 wherein the TMDC is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems, by selectively transmitting the TMV that is received to the at least one of the target computer systems if the TMV applies to the at least one of the target computer systems.

3. A system according to Claim 1 wherein the TMDC is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems, by selectively transmitting selected fields in the TMV that is received to the at least one of the target computer systems.

4. A system according to Claim 1 wherein the TMDC is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target systems in the domain of target computer systems, by mutating the TMV that is received to a format that is compatible with the at least one of the computer systems in the domain of target systems.

5. A system according to Claim 1 wherein the TMDC is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target systems in the domain of target computer systems, by transmitting to the selected one of the target computer systems, the TMV, including a Program Instance (PI) vector that identifies a program instance at a selected one of the target computer systems.

6. A system according to Claim 1 wherein the TMDC is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target systems in the domain of target computer systems, by having a TMV generator generate a TMV Generation Number (TMVGN) that tracks TMVs that are processed by the TMDC and by using the TMVGN to control transmitting of TMVs that were not previously transmitted to a program instance at a target computer system due to unavailability of the program instance, upon availability of the program instance.

7. A system according to Claim 1 wherein the TMDC further comprises a Domain Store and Forward Repository (DSFR) that is configured to store a TMV until the TMV has been provided to all program instances in the domain of target computer systems and to purge the TMV thereafter.

8. A system according to Claim 1 wherein the at least one of the target systems comprises a plurality of program instances, and wherein the at least one of the target systems is configured to register the plurality of program instances with the TMDC.

9. A system according to Claim 8 wherein each of the program instances is configured to register with the TMDC, and to reregister with the TMDC upon reinstatiation.

10. A system according to Claim 8 wherein the TMDC further comprises a target system control system that is configured to register the plurality of program instances in the target system with the TMDC.

11. A system according to Claim 8 wherein the TMDC is further configured to obtain missing TMV information and to transmit the missing TMV information to the at least one of the target systems during registration of the plurality of program instances with the TMDC.

12. A system according to Claim 1 wherein the system type comprises a computer operating system type and/or an application program type.

13. A system according to Claim 1 further comprising a TMV generator that is configured to generate the TMV from a notification of a security threat that is received and to transmit the TMV to the TMDC.

14. A system according to Claim 13 wherein the TMV generator and the TMDC are further configured to synchronize TMV transmission therebetween such that all TMVs that are applicable to the domain of target systems are received by the TMDC.

15. A system according to Claim 1 wherein the target systems are configured to process the countermeasures that are identified in the processed TMV that is received from the TDMC.

16. A method for generating computer security threat management information, comprising:

receiving a computer-actionable Threat Management Vector (TMV) including therein a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat, a second computer-readable field that provides identification of a release level for the system type, and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level;

processing the TMV that is received for use by a domain of target computer systems; and

transmitting the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems.

17. A computer program product that is configured to generate computer security threat management information, the computer program product comprising a computer usable storage medium having computer-readable program code embodied in the medium, the computer-readable program code comprising:

computer-readable program code that is responsive to a computer-actionable Threat Management Vector (TMV), the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat, a second computer-readable field that provides identification of a release level for the system type, and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level, the computer-readable program code being configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in to the domain of target computer systems.

18. A computer program product according to Claim 17 wherein the computer-readable program code is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems, by selectively transmitting the TMV that is received to the at least one of the target computer systems if the TMV applies to the at least one of the target computer systems.

19. A computer program product according to Claim 17 wherein the computer-readable program code is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target computer systems in the domain of target computer systems, by selectively transmitting selected fields in the TMV that is received to the at least one of the target computer systems.

20. A computer program product according to Claim 17 wherein the computer-readable program code is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of

the target systems in the domain of target computer systems, by mutating the TMV that is received to a format that is compatible with the at least one of the target systems in the domain of target systems.

21. A computer program product according to Claim 17 wherein the computer-readable program code is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target systems in the domain of target computer systems, by generating a Program Instance (PI) vector that identifies a program instance at a selected one of the target computer systems and by transmitting the TMV, including the PI vector, to the selected one of the target computer systems.

22. A computer program product according to Claim 17 wherein the computer-readable program code is configured to process a TMV that is received for use by a domain of target computer systems and to transmit the TMV that has been processed to at least one of the target systems in the domain of target computer systems, by generating a TMV Generation Number (TMVGN) that tracks TMVs that are processed by the TMDC and by using the TMVGN to control transmitting of TMVs that were not previously transmitted to a program instance at a target computer system due to unavailability of the program instance, upon availability of the program instance.

23. A computer program product according to Claim 17 further comprising:

computer-readable program code that is configured to provide a Domain Store and Forward Repository (DSFR) that is configured to store a TMV until the TMV has been provided to all program instances in the domain of target computer systems and to purge the TMV thereafter.